

CLAIMS

What is claimed is:

1 1. A networked system for accessing information, comprising:
2 a first network station, representing a first network entity,
3 configured to control access to information stored on a network for
4 a third network entity, and to encrypt a first component message
5 with a first crypto-key associated with the first network entity;
6 a second network station, representing a second network
7 entity, configured to control access to the network by the third
8 network entity, to encrypt a second component message with a second
9 crypto-key, to combine the encrypted first and the encrypted second
10 component messages, and to transmit the combined messages over the
11 network; and

12 a third network station, representing the third network
13 entity, configured to receive the transmitted combined messages and
14 to further transmit the received combined messages over the network
15 in order to obtain access to the stored information;

16 wherein the first network station is further configured to
17 receive the further transmitted combined messages, to decrypt the
18 encrypted first and the encrypted second component messages in the
19 received further transmitted combined messages, and to control
20 access by the third network station to the stored information based
21 on the decrypted first and second component messages.

1 2. A networked system according to claim 1, wherein:
2 the first crypto-key is a symmetric crypto-key; and
3 the second crypto-key is a non-symmetric crypto-key.

1 3. A networked system according to claim 2, wherein:
2 the symmetric crypto-key is known only to the first network
3 entity.

1 4. A networked system according to claim 2, wherein;
2 the non-symmetric crypto-key is a private crypto-key of a
3 joint private-public crypto-key pair associated with the second
4 network entity.

1 5. A networked system according to claim 1, wherein:
2 the first crypto-key is a first non-symmetric crypto-key; and
3 the second crypto-key is a second non-symmetric crypto-key,
4 different than the first non-symmetric crypto-key.

1 6. A networked system according to claim 5, wherein:
2 the first non-symmetric crypto-key is a public crypto-key of
3 a joint private-public crypto-key pair associated with the first
4 network entity; and
5 the second non-symmetric crypto-key is a private crypto-key
6 of a joint private-public crypto-key pair associated with the
7 second network entity.

1 7. A networked system according to claim 1, wherein;
2 the first component message includes identity information
3 associated with the third network entity, and integrity information
4 which corresponds to the identity information; and
5 the second component message includes voucher information
6 which indicates that the second network entity has authenticated
7 the third network entity.

1 8. A networked system according to claim 1, further comprising:
2 a fourth network station, representing a fourth network
3 entity, configured to encrypt a third component message with a
4 third crypto-key, to initially combine the encrypted first and the
5 encrypted third component messages, and to transmit the initially
6 combined messages over the network;

7 wherein the second network station is further configured to
8 receive the transmitted initially combined messages, to combine the
9 encrypted first and the encrypted third component messages in the
10 received initially combined messages with the encrypted second
11 component message to create the combined messages;

12 wherein the first network station is further configured to
13 decrypt the encrypted third component message in the received
14 further transmitted combined messages, and to control access by the
15 third network station to the stored information based also on the
16 decrypted third component message.

1 9. A networked system according to claim 8, wherein:

2 the first component message includes identity information
3 associated with the third network entity, and integrity information
4 which corresponds to the identity information;

5 the second component message includes voucher information
6 which indicates that the second network entity has authenticated
7 the third network entity; and

8 the third component message includes relationship information
9 which indicates that the identity and the integrity information was
10 received by the fourth network entity from the first network entity
11 and transmitted by the fourth network entity to the second network
12 entity.

1 10. A networked system according to claim 8, wherein:

2 the first crypto-key is a symmetric crypto-key;

3 the second crypto-key is a non-symmetric crypto-key; and

4 the third crypto-key is a non-symmetric crypto-key.

1 11. A networked system according to claim 1, wherein:

2 the second component message further includes a timestamp
3 corresponding to a time at which the combined messages are
4 transmitted by the second network station.

1 12. A networked system according to claim 1, wherein:

2 the first network station is further configured to combine the
3 encrypted first component message with a network address for the
4 stored information;

5 the second network station is further configured to combine
6 the combined encrypted first component message and the network
7 address with the encrypted second component message to create the
8 combined messages; and

9 the first network station is further configured to control
10 access by the third network station to the stored information based
11 on the network address and the decrypted first and second component
12 messages.

13. A networked system according to claim 1, wherein:

14 the second network station transmits the combined message in
15 response to a received request;

16 the first network station encrypts the first component message
17 prior to receipt of the request by the second network station; and

18 the second network station encrypts the second component
19 message and combines the encrypted first and the encrypted second
20 component messages after receipt of the request by the second
21 network station.

1 14. A method of creating an electronic message for transmission
2 over a network, comprising the steps of:

3 encrypting a first component with a first crypto-key,
4 associated with a first network entity, such that the encrypted
5 first component can be decrypted by only the first network entity;

6 encrypting a second component with a second crypto-key,
7 associated with a second network entity, such that the encrypted
8 second component can be decrypted by the first network station; and
9 transmitting the encrypted first component and the encrypted
10 second component as a combined message.

1 15. A method according to claim 14, wherein:
2 the first crypto-key is a symmetric crypto-key; and
3 the second crypto-key is a non-symmetric crypto-key.

1 16. A method according to claim 15, wherein:
2 the symmetric crypto-key is known only to the first network
3 entity; and
4 the non-symmetric crypto-key is known only to the second
5 network entity.

1 17. A method according to claim 15, wherein:
2 the non-symmetric crypto-key is a private crypto-key of a
3 joint private-public crypto-key pair associated with the second
4 network entity.

1 18. A method according to claim 14, wherein:
2 the first crypto-key is a first non-symmetric crypto-key; and
3 the second crypto-key is a second non-symmetric crypto-key.

1 19. A method according to claim 18, wherein:
2 the first non-symmetric crypto-key is a public crypto-key of
3 a joint private-public crypto-key pair associated with the first
4 network entity; and
5 the second non-symmetric crypto-key is a private crypto-key
6 of a joint private-public crypto-key pair associated with the
7 second network entity.

1 20. A method according to claim 14, further comprising the steps
2 of:

3 encrypting a third component with a third crypto-key,
4 associated with a third network entity, such that the encrypted
5 third component can be decrypted by the first network entity; and
6 transmitting the encrypted third component with the encrypted
7 first and the encrypted second components as the combined message.

1 21. A method according to claim 20, wherein:

2 the first crypto-key is a symmetric crypto-key;
3 the second crypto-key is a first non-symmetric crypto-key;
4 and
5 the third crypto-key is a second non-symmetric crypto-key.

11 22. A method according to claim 20, wherein:

12 the first component includes identity information associated
13 with a fourth network entity and integrity information
14 corresponding to the identity information;

15 the second component includes relationship information which
16 indicates that the identity and the integrity information were
17 received by the second network entity from the first network entity
18 and transmitted by the second network entity to the third network
19 entity; and

20 the third component includes voucher information which
21 indicates that the third network entity authenticated the fourth
22 network entity.

1 23. A method according to claim 20, wherein:

2 the third component further includes a timestamp corresponding
3 to a time at which the combined message is transmitted to the
4 fourth network entity.

1 24. A method according to claim 20, further comprising the step of:
2 transmitting the encrypted first, the encrypted second and the
3 encrypted third components with a network address as the combined
4 message.

1 25. A method according to claim 14, wherein:
2 the combined message is transmitted responsive to a received
3 request;
4 the first component is encrypted prior to receipt of the
5 request; and
6 the second component is encrypted after receipt of the
7 request.

1 26. An electronic message, comprising:
2 a first component created by a first network entity and
3 encrypted with a first crypto-key, associated with the first
4 network entity, such that the encrypted first component can be
5 decrypted by only the first entity; and
6 a second component created by a second network entity, and
7 encrypted with a second crypto-key, such that the encrypted second
8 component can be decrypted by the first network entity.

1 27. An electronic message according to claim 26, wherein:
2 the first crypto-key is a symmetric crypto-key known only to
3 the first network entity; and
4 the second crypto-key is a non-symmetric crypto-key.

1 28. An electronic message according to claim 27, wherein;
2 the non-symmetric crypto-key is a private crypto-key of a
3 joint private-public crypto-key pair associated with the second
4 network entity.

1 29. An electronic message according to claim 26, wherein:
2 the first crypto-key is a first non-symmetric crypto-key; and
3 the second crypto-key is a second non-symmetric crypto-key.

1 30. An electronic message according to claim 29, wherein:
2 the first non-symmetric crypto-key is a public crypto-key of
3 a joint private-public crypto-key pair associated with the first
4 network entity; and
5 the second non-symmetric crypto-key is a private crypto-key
6 of a joint private-public crypto-key pair associated with the
7 second network entity.

2 31. An electronic message according to claim 26, further
3 comprising:

4 a third component created by a third network entity and
5 encrypted with a third crypto-key, associated with the third
6 network entity, such that the encrypted third component can be
7 decrypted by the first network entity.

2 32. An electronic message according to claim 31, wherein:
3 the first component includes identity information associated
4 with a fourth network entity, and integrity information
5 corresponding to the identity information;

5 the second component includes relationship information which
6 indicates that the identity and the integrity information were
7 received by the second network entity from the first network entity
8 and transmitted by the second network entity to the third network
9 entity; and

10 the third component includes voucher information which
11 indicates that the third network entity has authenticated the
12 fourth network entity.

1 33. An electronic message according to claim 32, wherein:
2 the integrity information includes a hash of the identity
3 information.

1 34. An electronic message according to claim 32, wherein:
2 the third component further includes a timestamp corresponding
3 to a time at which the electronic message is transmitted by the
4 third network entity to the fourth network entity.

1 35. An electronic message according to claim 26, wherein:
2 the first component includes identity information associated
3 with a third network entity;
4 the second component includes voucher information which
5 indicates that the second network entity has authenticated the
third network entity.

1 36. An electronic message according to claim 35, wherein:
2 the second component further includes a timestamp
3 corresponding to a time at which the electronic message is
4 transmitted by the second network entity to the third network
entity.

1 37. An electronic message according to claim 26, wherein:
2 the first network entity controls access to information
3 available on a network; and
4 the second entity controls access to other network entities.

1 38. An electronic message according to claim 26, wherein the first
2 component includes an identification of information stored on a
3 network, and further comprising:
4 a network address at which the identified stored information
5 can be accessed.

1 39. An electronic message, comprising:
2 a first component encrypted with only a symmetric crypto-key;
3 and
4 a second component, different than the first component,
5 encrypted with only a non-symmetric crypto-key.

1 40. An electronic message according to claim 39, wherein:
2 the symmetric crypto-key is associated with a first entity;
3 and
4 the non-symmetric crypto-key is associated with a second
5 entity.

1 41. An electronic message according to claim 40, wherein:
2 the symmetric crypto-key is known only to the first entity.

1 42. An electronic message according to claim 40, wherein;
2 the non-symmetric crypto-key is a private crypto-key of a
3 joint private-public crypto-key pair associated with the second
4 entity.

1 43. An extended network universal resource locator, comprising:
2 a first component including a network address at which stored
3 information can be accessed on a network;
4 a second component including identity information associated
5 with a first network entity and an integrity value corresponding
6 to the identity information, the second component being encrypted
7 with a first crypto-key of a second network entity; and
8 a third component including voucher information indicating
9 that a third network entity has authenticated the first network
10 entity and that transmission of the extended network universal
11 resource locator by the third network entity to the first network

12 entity occurred at a particular time, the third component being
13 encrypted with a second crypto-key of the third network entity.

1 44. An extended universal resource locator according to claim 43,
2 further comprising:

3 a fourth component including relationship information
4 indicating that the encrypted second component was received by a
5 fourth network entity from the second network entity and
6 transmitted by the fourth network entity to the third network
7 entity, the fourth component being encrypted with a third crypto-
8 key of the fourth network entity.

1 45. An extended universal resource locator according to claim 44,
2 wherein:

3 the first crypto-key is a symmetric crypto-key known only to
4 the second network entity;

5 the second crypto-key is a first non-symmetric crypto-key
6 associated with the third network entity; and

7 the third crypto-key is a second non-symmetric crypto-key
8 associated with the fourth network entity.

1 46. An extended universal resource locator according to claim 45,
2 wherein;

3 the first non-symmetric crypto-key is one of a private crypto-
4 key and a public crypto-key of a joint private-public crypto-key
5 pair associated with the third network entity; and

6 the second non-symmetric crypto-key is one of a private
7 crypto-key and a public crypto-key of a joint private-public
8 crypto-key pair associated with the fourth network entity.

1 47. An extended universal resource locator according to claim 44,
2 wherein:

3 the stored information is detailed bill information;
4 the network address is an Internet URL;
5 the identity information includes an identification of the
6 stored information and an account number associated with the first
7 network entity;
8 the integrity value is a hash of the identity information; and
9 the transmission time information is a timestamp.

1 48. An extended universal resource locator according to claim 44,
2 wherein:

3 the second network entity controls access to the stored
4 information;

5 the fourth network entity controls access to other information
6 which is transmitted with the extended network universal resource
7 locator by the third network entity to the first network entity;
8 and

9 the third network entity controls access by the first network
10 entity to other network entities.

11 49. An extended universal resource locator according to claim 48,
12 wherein:

13 the stored information is detailed bill information associated
14 with the first entity; and

15 the other information is summary bill information associated
16 with the first network entity.